Lab Assignment 6 – Cryptography – PGP and SSL

Lab Write-up (write a few sentences on each)

1. What is PGP?

PGP stands for Pretty Good Privacy. It is an encryption method that lets you communicate privately online. It basically takes anything you put into it and turns it into ciphertext, and it enables you to give the recipient a key so only the person with that key can decrypt the message. This provides both privacy and authentication because if you are encrypting and decrypting with that key, and you know where that key came from, then you know that's where the encrypted text came from.

2. How does PGP work?

So PGP works by putting whatever you're looking to encrypt into an algorithm and then changes that into ciphertext and only the person with the key can decrypt it and read it. PGP uses public key encryption which is known as asymmetric encryption as well as symmetric key encryption.

3. What is a digital signature?

A digital signature is a way to prove to the recipient that an attacker has not manipulated the message in any way. You get your digital signature by using the sender's private key on a mathematical hash of the plain text message. This signature can be verified by using the sender's public key, and if the message has been altered in any way, the signature will be invalid.

4. Define symmetric and asymmetric encryption?

Symmetric key encryption is where you use the same key to encrypt and decrypt the message this poses problems getting the key to the recipient in the first place because you don't want that key to be intercepted because with that key an attacker will be able to decrypt the message that you are sending through. Asymmetric encryption, also known as public key encryption, is the method of using a private key and a public key to encrypt data when you're sending it to an individual. You use the individual's public key to encrypt the messages and only the private key can decrypt that message. You are unable to use the public key to decrypt that message.

5. What is the primary difference between symmetric and asymmetric encryption?

The primary difference between symmetric and asymmetric encryption is with symmetric encryption you use the same key to encrypt and decrypt the message while with asymmetric encryption you use a key pair and you use the public key to encrypt and you use the private key to decrypt the message.

6. Why is asymmetric (Public/Private Key) encryption better for securing data with a previously unknown party?

The main reason that public key is better for dealing with someone that you haven't dealt with before is because you don't want to give away your private key when it comes to symmetric encryption because then they may be able to decrypt other messages that you sent using that same key. With Public Key Encryption you use a public key and those keys are public so it doesn't matter if they have it or not they can't do anything with it other than encrypt a message just sent to you.

7. What is an SSL certificate?

An SSL certificate is a digital certificate that basically tells you the identity of the website and enables encrypted communication with them because it contains their public key. It also contains the domain name, the certificate's expiration date, and the certificate authority that issued it. If the site has a valid SSL certificate, it basically tells you that the site is legitimate, that you can encrypt your data and send it, and that the connection is safe.

8. How does SSL encryption work?

So SSL encryption is a multi-step process that your browser does in the background in order to create a secure connection between you and the website that you're trying to access. The first step your browser connects to the website and requests its SSL certificate once it receives that from them it then goes to a certificate authority and verifies that certificate is valid if the certificate is valid your browser will then generate A symmetric key for that particular connection you then send that session key to the website using the website it's public key which is included in the SSL certificate and then once they have that key they can then encrypt a message to send back to you with their own symmetric key and that ensures a faster connection because symmetric is faster than asymmetric encryption so it just makes it a little bit quicker.

9. Where would I use an SSL certificate?

The main places you're going to want to use an SSL certificate are anywhere you want to prove the website's identity and encrypt data between you and the site. This includes anything dealing with logins, e-commerce sites, and any site that collects personal information, such as HR portals and similar systems. You'll also want to use SSL for e-mail and e-mail services. Basically, you need an SSL certificate anywhere you want secure connections so people can't eavesdrop on your communications and anywhere you want to maintain authentication and privacy.

Deliverable: Compile you answers in your lab write-up.

Deliverable:

1. Gather the deliverables listed for each task
2. Name the pdf CTI2318-Lab6-Firstname-lastname.pdf where first name is your first name and last name is your last name
3. Upload the pdf to FSO in the appropriate area for Lab 6

Grading Rubric:

- ✓ **All Questions fully answered w/ 2 sentences + Critical Thinking: 81/81 points**
- ✓ **Proofreading + Spelling/Punctuation/Grammar: 10/10 points**
- ✓ **All Upload Instructions Followed: 9/9 points**